REMARKS/ARGUMENTS

Claims 1-48 are pending. Claims 49-50 were previously canceled. Claims 1-25 were previously withdrawn from consideration. Claims 26-48 were rejected under 35 U.S.C. 103(a) as being unpatentable over Hawes (USPN 5,070,528) in view of Hagerman (USPN 6,973,568).

Rejections under 35 U.S.C. 112

Claims 36-48 were rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. To facilitiate prosecution, independent claims 36 and 48 have been amended to recite "a [[the]] security enable parameter" in response to the Examiner's suggestion.

Rejections under 35 U.S.C. 103(a)

All currently pending and non-withdrawn claims were rejected under 35 U.S.C. 103(a) as being unpatentable over Hawes (USPN 5,070,528) in view of Hagerman (USPN 6,973,568). These rejections are respectfully traversed.

Various embodiments provide techniques for improving security in a fibre channel network. Among other things, the techniques involve use of a "security enable parameter", a "security control indicator" and/or a "security association identifier", to facilitate authentication and other security related functions, each such parameter/ indicator/identifier serving a particular function as recited in the claims. The "security *enable* parameter" allows for two network nodes to authenticate one another. For example, in some embodiments, when a network entity is introduced into a fibre channel fabric, the new node transmits a "security enable parameter" along with the initialization message. If the receiving node supports authentication or other security features, the receiving node can extract the security enable parameter and transmit an acknowledgment message that it supports security features. *See* independent claim 26. (*See also* Specification: Page 11, lines 20-27). As recited in the claims, such acknowledgement message "includ[es] algorithm information and a salt parameter". A salt parameter is generally used to make passwords more secure, and is described in detail in the Specification. (See Specification, page 12).

With respect to the "security *control* indicator", the receiving node "identif[ies] a security control indicator in [a] second frame", where the security control indicator "is used to

determine if the second frame is encrypted or authenticated". Please note, as distinct from the security enable parameter discussed above, the security control indicator addresses authentication or encryption of a particular frame, not authentication of a node.

With respect to the "security *association* identifier", the receiving node "determin[es] that a security association identifier associated with the second frame corresponds to an entry in a security database" and "decrypt[s] a first portion of the second frame by using algorithm information contained in the entry in the security database."

The Applicants respectfully submit that independent claims 26, 36 and 48, as amended, are not obvious over the combined teachings of Hawes and Hagerman.

Hawes describes techniques for improving processing of information packets that require cryptographic processing by providing ways to "avoid having to parse each information packet in detail and to account for differences in protocol and packet formats". Hawes accomplishes this result by including in "each packet that is to be cryptographically processed" "a special cryptographic preamble, which contains an offset specifying the location of the data to be processed, and a complete definition of the type of processing to be employed" on that packet.

> "More specifically, the offset field included in the cryptographic preamble indicates a number of data elements to skip to the start of the material to be cryptographically processed. In the method of the invention, this offset is used to skip over header information in the packet, which may vary in length and content depending on the protocol under which the packet was generated."
>
> "The cryptographic preamble further includes a mode field indicating the type of cryptographic processing to be performed, and the step of performing the cryptographic processing includes conditioning the cryptographic processor to perform the type of processing requested in the mode field. The available modes include encrypting for outbound transmission, encrypting or decrypting for loopback to the node processor, encrypting a cipher key for loopback to the node processor, and computing an integrity check value for loopback to the node processor." (Hawes: column 6, lines 36-54)

Notably, Hawes is not concerned with determining whether a frame is one that requires cryptographic processing, much less determining whether a frame is authenticated or encrypted as recited in the claims. Hawes provides no teaching regarding how a determination is made that a frame is authenticated or encrypted. Rather, Hawes's focus is on adding information in a

packet's preamble to assist with such cryptographic processing *in the event that* cryptographic processing is needed. (Hawes: Column 6, lines 9-20, Abstract).

In contrast, the claims of the present application teach a process for a first node to determine whether a second node has "authentication capability or supports other security functions" by sending a message to the receiving node with a "security enable parameter". As noted above, the receiving node then responds with a message acknowledging that it has such capability. The claims also specify that such acknowledgement messages also include "algorithm information and a salt parameter". As described in the specification, the salt parameter is used in forming secure passwords. Hawes makes no mention of algorithms or salt parameters.

Further, Hawes makes no mention of a security database that contains entries, each entry corresponding to a security association identifier and containing an algorithm that can be used to "decrypt" a portion of any frames containing the security association identifier in the manner claimed.

The sections of Hawes referenced by the Examiner do not teach authentication of a node, among other things. Instead, they specifically teach "authentication" or "integrity" of a message (i.e., that a message has not been tampered with) or "confidentiality" of a message (i.e., that message contents are not divulged in transit). (Hawes, Column 3, lines 29-36). The Examiner analogizes the recited "security enable parameter" to the "preamble" of Hawes's packets, stating: "it is this preamble that the Examiner has equated with Applicant's 'security enable indicator' because it allows a system to determine *whether a particular packet has been encrypted and how* so that the necessary actions may be taken thereupon". (Office Action, page 2-3 (emphasis added)). However, the security enable parameter recited in the claims is not used to "determine whether a particular packet has been encrypted", as the Examiner suggests in the above statement. Instead, the security enable parameter is used to allow a storage area network node to authenticate, or establish a secure channel with, another node.

Hagerman fails to cure the deficiencies of Hawes.

Hagerman describes techniques for implementing spoofing-and replay-attack-resistant virtual zones on storage area networks. It does this by including at each port of the storage area

network nodes "a hash function generator for providing and verifying an authentication code for frames transmitted over the storage area network, and a key table for providing a key to the hash function generator." "The authentication code is generated by applying a hash function to the key and to at least an address portion of each frame. In each node, the key is selected from that node's key table according to address information of the frame." (Hagerman, Abstract). Hagerman states "The key value used to compute the authentication code field 300 is extracted from a key table 170, 172, 174, 176, 178, and 180 associated with each port. These key tables may be, and often are, dissimilar from port to port, for example key table 170 need not be the same as key table 172. The key tables are initialized such that the key table associated with a given port contains keys for communication with the ports that the given port is authorized to communicate with. For example, if port 130 is authorized to communicate through port 138 and storage system 110 to logical unit 114, key table 170 associated with port 130 and key table 178 associated with port 138 will have at least one common key for port 138--port 130 communications. If port 132 is not authorized to communicate with port 138, then key table 172 and key table 178 will not have a common key for port 132--port 138 communications." (Figure 3 Description)

The sections of Hagerman referenced by the Examiner do not teach a process for using a security enable parameter, a security control indicator, or a security association identifier, to perform security related functions. Nor do they teach the techniques for node and message authentication and security recited in the claims. Instead, they specifically teach the use of virtual zones to protect against spoofing and replay-attacks. The virtual zones are organized by key values tables on each node of the storage area network, and these key value tables "preferably contain[] unique key values for each node pair of the SAN between which communications are permitted". (Hagerman, Column 3, lines 34-47).

Independent claims 26, 36 and 48 have been amended to further clarify the invention, for the purpose of advancing prosecution of the present application. The amendments are supported by the specification, for example, at page 11, line 18, to page 12, line 12. As the Applicants believe the claims to be patentable over the art of record as set forth in the foregoing arguments, these amendments are not being presented for any reason related to patentability.

In view of the foregoing, Applicants believe all rejections have been overcome thereby placing all independent and dependent claims now pending in this application in condition for

allowance. If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at the number provided below.

Respectfully submitted,
Weaver Austin Villeneuve & Sampson LLP

/Audrey Kwan/

G. Audrey Kwan
Reg. No. 46,850

P.O. Box 70250
Oakland, CA 94612-0250
(510) 663-1100
gak/scm